

STAGE 1 REPORT

Vulnerability Analysis on OWASP Top 10

Part 1: Executive Summary

1. Overview

Cybersecurity protects digital systems, networks, and data from unauthorized access, attacks, damage, or theft. In an increasingly digital and interconnected world, cybersecurity plays a critical role in ensuring the confidentiality, integrity, and availability of information and systems. It encompasses a wide range of technologies, processes, and practices designed to safeguard digital assets and mitigate the risks posed by cyber threats.

The OWASP Top 10 list aims to highlight the ten most critical and prevalent security risks in web applications and software systems. This list serves as a valuable resource for developers, security professionals, and organizations to prioritize their efforts and focus on addressing the most significant security vulnerabilities that could potentially be exploited by attackers. By raising awareness about these common risks, the OWASP Top 10 aims to guide the implementation of effective security measures, best practices, and mitigation strategies to build more secure and resilient applications.

Common Weakness Enumeration (CWE) is a community-developed list of common software security weaknesses or vulnerabilities. It provides a standardized way to categorize and describe common security issues that can arise in software systems, applications, and code. Each weakness in the CWE list is assigned a unique identifier and includes a detailed description of the vulnerability, its potential impact, and guidance on preventing or mitigating it. CWE helps developers, security professionals, and organizations identify, understand, and address security weaknesses in their software, leading to more secure and robust applications.

In this project we are going to identify the CWE references for each OWASP top 10 vulnerabilities. For each vulnerability

2. List of Vulnerable Parameter, Location discovered

S. No.	Name of The Vulnerability	References-CWE
A01	Broken Access Control	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
A02	Cryptographic Failures	CWE-325: Missing Cryptographic Step
A03	Injection	CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')
A04	Insecure Design	CWE-257: Storing Passwords in a Recoverable Format
A05	Security Misconfiguration	CWE-11: ASP.NET Misconfiguration: Creating Debug Binary
A06	Vulnerable and Outdated Components	CWE-1104: Use of Unmaintained Third Party Components
A07	Identification and Authentication Failures	CWE-290: Authentication Bypass by Spoofing
A08	Software and Data Integrity Failures	CWE-494: Download of Code Without Integrity Check
A09	Security Logging and Monitoring Failures	CWE-532: Insertion of Sensitive Information into Log File
A10	Server-Side Request Forgery	CWE-918: Server-Side Request Forgery (SSRF)

3. Vulnerability Details – CWE

1 . Vulnerability Name: Exposure of Sensitive Information to an Unauthorized Actor

CWE : CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

OWASP Category: A01:2021 – Broken Access Control

Description: The product reveals confidential data to an entity that lacks explicit authorization to access such information.

Business Impact: The exposure of sensitive information to an unauthorized actor can have severe business consequences, including potential legal liabilities, loss of customer trust, financial penalties, and a negative impact on the company's brand reputation. This breach could also disrupt normal operations, require costly mitigation efforts, and necessitate implementing stricter security measures to prevent future incidents.

2 . Vulnerability Name: Missing Cryptographic Step

CWE : CWE-325: Missing Cryptographic Step

OWASP Category: A02:2021 –Cryptographic Failures

Description: The product does not implement a required step in a cryptographic algorithm, resulting in weaker encryption than advertised by the algorithm.

Business Impact: A missing cryptographic step in a process or system can result in compromised data integrity and confidentiality. This vulnerability might lead to unauthorized access, data manipulation, and breaches, potentially causing substantial financial losses, legal liabilities, damaged customer trust, and harm to the company's reputation. Rapid remediation and security enhancement measures would be imperative to address such a critical lapse.

3 . Vulnerability Name: Improper Neutralization of Special Elements used in a Command

CWE : CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

OWASP Category: A03:2021 –Injection

Description: The product constructs all or part of a command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended command when it is sent to a downstream component.

Business Impact: Failing to properly neutralize special elements within a command can have serious business ramifications. This vulnerability may allow attackers to execute malicious commands, potentially leading to unauthorized data exposure, system disruption, and even complete compromise. As a result, sensitive information might be stolen, operations could be severely impacted, customer trust could erode, and the company could face financial losses, legal actions, and reputational damage. Swift corrective actions and reinforced security protocols would be essential to mitigate this risk effectively.

4 . Vulnerability Name: Storing Passwords in a Recoverable Format

CWE : CWE-257: Storing Passwords in a Recoverable Format

OWASP Category: A04:2021 – Insecure Design

Description: The storage of passwords in a recoverable format makes them subject to password reuse attacks by malicious users. In fact, it should be noted that recoverable encrypted passwords provide no significant benefit over plaintext passwords since they are subject not only to reuse by malicious attackers but also by malicious insiders. If a system administrator can recover a password directly, or use a brute force search on the available information, the administrator can use the password on other accounts.

Business Impact: Storing passwords in a recoverable format poses significant business risks. If such a vulnerability is exploited, it could lead to unauthorized access, data breaches, and compromised user accounts. This breach of security might result in legal consequences, loss of customer trust, financial penalties, and reputational harm for the company. Ensuring passwords are securely hashed

and encrypted is crucial to prevent these potential consequences and maintain a strong security posture.

5 . Vulnerability Name: ASP.NET Misconfiguration: Creating Debug Binary

CWE : CWE-11: ASP.NET Misconfiguration: Creating Debug Binary

OWASP Category: A05:2021 – Security Misconfiguration

Description: Debugging messages help attackers learn about the system and plan a form of attack.

Business Impact: This oversight may expose sensitive source code and internal system details, making it easier for attackers to identify vulnerabilities and potentially leading to unauthorized system access and data breaches. The resulting consequences could include intellectual property theft, customer data exposure, operational disruptions, legal liabilities, financial losses, and damage to the company's reputation. It is vital to ensure proper configuration and deployment practices to mitigate these risks effectively.

6. Vulnerability Name: Use of Unmaintained Third Party Components

CWE : CWE-1104: Use of Unmaintained Third Party Components

OWASP Category: A06:2021 – Vulnerable and Outdated Components

Description: The product relies on third-party components that are not actively supported or maintained by the original developer or a trusted proxy for the original developer.

Business Impact: These components may contain vulnerabilities that can be exploited by attackers, potentially leading to security breaches, data compromises, and system failures. Such incidents could result in financial losses, regulatory non-compliance, legal actions, erosion of customer trust, and damage to the company's reputation. Regularly updating and monitoring third-party components is crucial to minimize these risks and maintain a robust security posture.

7. Vulnerability Name: Authentication Bypass by Spoofing

CWE : CWE-290: Authentication Bypass by Spoofing

OWASP Category: A07:2021 – Identification and Authentication Failures

Description: This attack-focused weakness is caused by incorrectly implemented authentication schemes that are subject to spoofing attacks.

Business Impact: Attackers exploiting this vulnerability can gain unauthorized access to systems, applications, or data by disguising their identity. This could lead to data breaches, compromised user accounts, unauthorized transactions, and even system manipulation or disruption. The resulting impact might include financial losses, regulatory penalties, legal liabilities, customer distrust, and damage to the company's reputation. Implementing strong authentication mechanisms and continuous monitoring are essential to prevent and mitigate the risks associated with authentication spoofing.

8. Vulnerability Name: Download of Code Without Integrity Check

CWE : CWE-494: Download of Code Without Integrity Check

OWASP Category: A08:2021 – Software and Data Integrity Failures

Description: The product downloads source code or an executable from a remote location and executes the code without sufficiently verifying the origin and integrity of the code.

Business Impact: This vulnerability exposes systems to the risk of malicious code injection, which can lead to unauthorized access, data breaches, system instability, and compromised functionalities. These outcomes could result in financial losses, regulatory violations, legal liabilities, reputational damage, and erosion of customer trust. Ensuring robust code validation and integrity checks before downloading is crucial to mitigate potential risks and uphold a strong security posture.

9. Vulnerability Name: Insertion of Sensitive Information into Log File

CWE : CWE-532: Insertion of Sensitive Information into Log File

OWASP Category: A09:2021 – Security Logging and Monitoring Failures

Description: Information written to log files can be of a sensitive nature and give valuable guidance to an attacker or expose sensitive user information.

Business Impact: This lapse could expose confidential data, such as user credentials or proprietary details, potentially leading to unauthorized access, data breaches, and regulatory non-compliance. These consequences might result in financial losses, legal liabilities, tarnished reputation, and erosion of customer trust. Implementing proper log management practices, including sanitization of sensitive information, is crucial to mitigate these risks and maintain data security and compliance.

10. Vulnerability Name: Server-Side Request Forgery (SSRF)

CWE : CWE-918: Server-Side Request Forgery (SSRF)

OWASP Category: A10:2021 – Server-Side Request Forgery

Description: The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination.

Business Impact: Attackers exploiting SSRF can manipulate a server into making unauthorized requests to other internal resources or external services, potentially leading to data breaches, unauthorized access, and even remote code execution. This could result in compromised systems, customer data exposure, financial losses, regulatory penalties, legal actions, and damage to the company's reputation. Implementing robust input validation, network segmentation, and security controls is critical to preventing and mitigating the risks associated with SSRF vulnerabilities.

STAGE 2 REPORT

NESSUS Vulnerability Assessment Report

Overview :

Nessus is a powerful tool for vulnerability assessment, it should be used in conjunction with other security practices, such as penetration testing and regular security updates, to maintain a robust security posture. It helps organizations identify and address security vulnerabilities in their IT infrastructure, applications, and network systems.

Key Features of Nessus:

Vulnerability Scanning: Nessus scans networks, systems, and applications for vulnerabilities. It can identify common security issues such as misconfigurations, outdated software, weak passwords, and known software vulnerabilities.

Extensive Plugin Library: Nessus uses a vast and continuously updated database of plugins to perform scans. These plugins contain vulnerability checks and provide detailed information about potential risks.

Scanning Capabilities: Nessus offers a range of scanning options, including network scans, host-based scans, web application scans, and more. It can perform both authenticated scans (using valid credentials) and unauthenticated scans.

Policy Compliance: Nessus can assess systems against security policies and compliance standards (such as PCI DSS, HIPAA, and CIS benchmarks). This helps organizations ensure that their systems adhere to industry regulations and best practices.

Reporting: After completing a scan, Nessus generates comprehensive reports detailing the vulnerabilities found, their severity, and recommendations for remediation. These reports can be customized and shared with relevant stakeholders.

Risk Prioritization: Nessus assigns severity levels to vulnerabilities, helping organizations prioritize which issues need to be addressed urgently based on potential impact and exploitability.

Integration: Nessus can integrate with other security tools and solutions, such as Security Information and Event Management (SIEM) systems, to provide a more holistic view of an organization's security landscape.

Continuous Monitoring: Nessus can be configured to perform regular scans on a scheduled basis, enabling organizations to identify and address new vulnerabilities as they emerge.

User Management: Nessus supports user authentication and access controls, allowing different team members to have different levels of access to the tool's features and scan results.

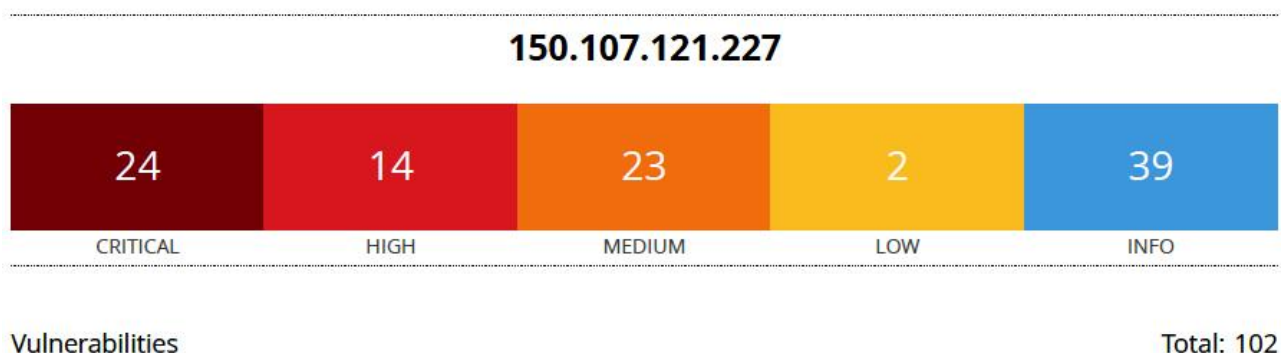
API and Automation: Nessus provides an API that allows for automation of scanning tasks, integration with other tools, and custom reporting.

Cloud and Container Support: In addition to on-premises systems, Nessus can scan cloud environments and containerized applications to ensure consistent security across different platforms.

Target website: <https://www.ritchennai.org/>

Target IP Address: 150.107.121.227

Nessus Result Summary:



List of Vulnerability:

S.No.	Vulnerability Name	Severity	Plugins
1	Apache 2.4.x < 2.4.33 Multiple Vulnerabilities	CRITICAL	122060
2	Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF	CRITICAL	156255
3	OpenSSL 1.0.2 < 1.0.2ze Vulnerability	CRITICAL	160480
4	PHP 7.1.x < 7.1.15 Stack Buffer Overflow	CRITICAL	107218
5	OpenSSL 1.0.2 < 1.0.2zd Vulnerability	HIGH	158973
6	SSL Medium Strength Cipher Suites Supported (SWEET32)	HIGH	42873
7	TLS Version 1.0 Protocol Detection	MEDIUM	104743
8	PHP 7.1.x < 7.1.22 Transfer-Encoding Parameter XSS Vulnerability	MEDIUM	117499
9	Ethernet Card Manufacturer Detection	INFO	35716
10	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	INFO	46215

REPORT

1. Vulnerability Name: Apache 2.4.x < 2.4.33 Multiple Vulnerabilities

Severity : CRITICAL

Plugin: 122060

Port : 80

Description: The remote web server is affected by multiple vulnerabilities. According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.33. It is, therefore, affected by multiple vulnerabilities

Solution: Upgrade to Apache version 2.4.33 or later.

Business Impact: There are several security problems or weaknesses in a software called Apache, which is used to run websites and web applications. These vulnerabilities could potentially harm a business in various ways, such as:

- **Data Breach:** Attackers may exploit these weaknesses to gain unauthorized access to sensitive data, leading to data breaches and privacy violations.
- **Website Downtime:** Exploiting these vulnerabilities can cause a website to crash or become unavailable to users, resulting in downtime and lost business opportunities.
- **Loss of Customer Trust:** Security issues can erode customer trust in a business, as users may worry about the safety of their information on the website.
- **Financial Costs:** Remediating these vulnerabilities and recovering from security incidents can be expensive, potentially requiring investment in cybersecurity measures and legal actions.
- **Reputation Damage:** A security breach can harm a company's reputation, making it less attractive to customers and partners.

These vulnerabilities in Apache software pose risks to the security, reliability, and reputation of a business that relies on it for its online presence. It's crucial to address these vulnerabilities promptly to mitigate these potential impacts.

2. Vulnerability Name: Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF

Severity : CRITICAL

Plugin: 156255

Port : tcp/80/

Description: The remote web server is affected by a denial of service or server-side request forgery vulnerability. The version of Apache httpd installed on the remote host is equal to or greater than 2.4.7 and prior to 2.4.52. It is, therefore, affected by a flaw related to acting as a forward proxy.

Solution: Upgrade to Apache version 2.4.52 or later.

Business Impact: This issue can affect a business in the following ways:

- **Service Disruption:** Attackers may exploit this problem to disrupt the normal operation of your website or online services. This disruption can lead to downtime, making your services unavailable to customers.
- **Data Exposure:** The security issue could allow attackers to access or manipulate data within your network, potentially leading to data breaches or unauthorized access to sensitive information.
- **Misuse of Resources:** Attackers might misuse your server's resources for their own purposes, causing increased server load and potentially higher hosting costs.
- **Reputation Damage:** Security vulnerabilities can harm your company's reputation. Customers may lose trust in your services if they perceive them as unreliable or insecure.
- **Legal and Compliance Issues:** Depending on the nature of the attack and the data involved, your business could face legal and compliance challenges, potentially resulting in fines or legal action.

3. Vulnerability Name: OpenSSL 1.0.2 < 1.0.2ze Vulnerability

Severity : CRITICAL

Plugin: 160480

Port : tcp/80/www

Description: The remote service is affected by a vulnerability. The version of OpenSSL installed on the remote host is prior to 1.0.2ze. It is, therefore, affected by a vulnerability as referenced in the 1.0.2ze advisory.

Solution: Upgrade to OpenSSL version 1.0.2ze or later.

Business Impact: There is a security problem in a software called OpenSSL, which is used to secure communications on the internet. This issue can impact a business in the following ways:

- **Data Security:** The vulnerability could potentially allow cyber attackers to intercept and compromise sensitive data, like customer information or financial transactions, that your business relies on for its operations.
- **Loss of Trust:** If customers or partners learn that your systems are vulnerable, they might lose trust in your business. They may worry about the security of their information when interacting with your website or services.
- **Service Disruption:** Exploiting this vulnerability can lead to service disruptions, making your website or online services unavailable to customers. This can result in lost revenue and customer frustration.
- **Reputation Damage:** Security issues can harm your company's reputation, making it less appealing to customers and partners. A damaged reputation can be difficult to recover from.
- **Legal and Compliance Issues:** Depending on the nature of the data involved and applicable regulations, your business could face legal and compliance challenges, including potential fines or legal action.

4. Vulnerability Name: PHP 7.1.x < 7.1.15 Stack Buffer Overflow

Severity : CRITICAL

Plugin: 107218

Port : tcp/80/www

Description: The version of PHP running on the remote web server is affected by a stack buffer overflow vulnerability. According to its banner, the version of PHP running on the remote web server is 7.1.x prior to 7.1.15. It is, therefore, affected by a stack buffer overflow vulnerability.

Solution: Upgrade to PHP version 7.1.15 or later.

Business Impact: This problem can affect a business in the following ways:

- **Security Breach:** Hackers may exploit this issue to gain unauthorized access to your website or web application. This can lead to data breaches, exposing sensitive information like customer data or business secrets.
- **Website Downtime:** Attackers exploiting this vulnerability can crash your website or make it temporarily unavailable to users. This downtime can result in lost sales and customer frustration.
- **Damage to Reputation:** Security problems can damage your business's reputation, making customers and partners hesitant to engage with your website or services due to concerns about security.
- **Financial Costs:** Fixing security vulnerabilities and recovering from attacks can be expensive, involving the cost of hiring experts, restoring systems, and potentially legal expenses.
- **Legal and Compliance Issues:** Depending on the nature of the breach and data involved, your business could face legal and compliance challenges, including potential fines or lawsuits.

5. Vulnerability Name: OpenSSL 1.0.2 < 1.0.2zd Vulnerability

Severity : HIGH

Plugin: 158973

Port : tcp/80/www

Description: The remote service is affected by a vulnerability. The version of OpenSSL installed on the remote host is prior to 1.0.2zd. It is, therefore, affected by a vulnerability as referenced in the 1.0.2zd advisory.

Solution: Upgrade to OpenSSL version 1.0.2zd or later.

Business Impact: The OpenSSL Vulnerability has significant potential business impacts. OpenSSL is a critical component used to secure online communications, and when vulnerabilities like this arise, they can have far-reaching consequences. First and foremost, this vulnerability could compromise the security of your data. Hackers may exploit it to gain unauthorized access to sensitive information, including customer data or proprietary business data. This could lead to data breaches, undermining customer trust and potentially causing regulatory and legal issues. Moreover, if customer data is exposed, your business could suffer reputation damage, which can be challenging to recover from, as customers and partners may hesitate to engage with your services due to security concerns.

Additionally, this vulnerability might result in service disruptions. If attackers exploit it, your website or online services could experience downtime, leading to lost revenue and customer frustration. The financial impact of remedying this vulnerability, including investing in cybersecurity measures and potentially facing legal expenses, can strain your budget. Legal and compliance concerns could also arise, especially if the compromised data is subject to regulations, potentially resulting in fines or legal consequences. In summary, addressing this OpenSSL vulnerability promptly is crucial to safeguard your business from potential data breaches, loss of trust, service disruptions, financial costs, and legal challenges.

6. Vulnerability Name: SSL Medium Strength Cipher Suites Supported (SWEET32)

Severity : HIGH

Plugin: 42873

Port : tcp/3389

Description: The remote service supports the use of medium strength SSL ciphers. The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Solution: Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Business Impact: This vulnerability might lead to service disruptions. If exploited, it can cause communication errors or slow down your systems, affecting the availability and performance of your website or online services. Such disruptions can lead to lost revenue, damage to your reputation, and customer frustration. In addition to these immediate consequences, addressing the SSL Medium Strength Cipher Suites Supported issue may also entail significant financial costs, including the expense of upgrading and securing your systems to eliminate the vulnerability. Overall, prompt action is essential to mitigate the potential business impacts of this vulnerability, including data breaches, loss of trust, service disruptions, financial burdens, and legal ramifications.

7. Vulnerability Name: TLS Version 1.0 Protocol Detection

Severity : MEDIUM

Plugin: 104743

Port : tcp/3389

Description: The remote service encrypts traffic using an older version of TLS. The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible. PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solution: Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Business Impact: This can have important business impacts:

- **Security Risk:** Using an old TLS version means that your data protection might not be strong enough. It's like having a weak lock on your business's front door. This could lead to data breaches and potentially harm your customers' trust.
- **Customer Frustration:** Some web browsers and services may not work well with old TLS versions, which could frustrate your customers. They might have trouble accessing your website or using your services, causing inconvenience.
- **Compliance Issues:** Depending on your industry and location, there might be rules and regulations that require you to use more up-to-date security. If you're not following these rules, you could face legal problems and fines.
- **Reputation Damage:** If customers hear that your website or service isn't secure, they might hesitate to do business with you. This could damage your company's reputation and make it harder to attract new customers.

8. Vulnerability Name: PHP 7.1.x < 7.1.22 Transfer-Encoding Parameter XSS Vulnerability

Severity : MEDIUM

Plugin: 117499

Port : tcp/80/www

Description: The version of PHP running on the remote web server is affected by a cross-site scripting vulnerability. According to its banner, the version of PHP running on the remote web server is 7.1.x prior to 7.1.22. It is, therefore, affected by a cross-site scripting vulnerability. An attacker could leverage this vulnerability to inject malicious code which executes within the security context of the affected site.

Solution: Upgrade to PHP version 7.1.22 or later.

Business Impact: This vulnerability in PHP, a widely used technology for web development, allows attackers to inject malicious code into your website or web application. Consequently, several detrimental business impacts may arise. Firstly, this

vulnerability can jeopardize the security of your website, potentially leading to unauthorized access, data breaches, or other cyberattacks. Such security breaches can not only damage your reputation but also result in financial losses due to legal and regulatory consequences, fines, and the costs associated with resolving the breach.

Secondly, customer trust is at stake. When visitors to your website discover that it's vulnerable to attacks like this, they may lose confidence in your business's ability to protect their data. This erosion of trust can result in a decline in customer loyalty and decreased engagement with your services. Moreover, the reputational damage stemming from this vulnerability may deter potential customers and partners from collaborating with your business, impacting growth opportunities. In summary, addressing the "PHP 7.1.x < 7.1.22 Transfer-Encoding Parameter XSS Vulnerability" is essential to mitigate the potential business impacts, including compromised security, loss of customer trust, reputational damage, financial burdens, and legal repercussions.

9. Vulnerability Name: Ethernet Card Manufacturer Detection

Severity : INFO

Plugin: 35716

Port : tcp/0

Description: The manufacturer can be identified from the Ethernet OUI. Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

Solution: n/a

Business Impact: This might not seem immediately concerning, but it can have some business impacts:

- **Security Risks:** Knowing the manufacturer could potentially help hackers find vulnerabilities or weaknesses in the network cards. This could lead to security breaches or unauthorized access to your company's network.
- **Information Leakage:** It might inadvertently reveal information about your technology infrastructure, which could be used by competitors or attackers to gain insights into your systems.

- **Competitive Advantage:** On the flip side, if your competitors can detect your Ethernet card manufacturer, they might gain insights into your technology choices, giving them a competitive edge.
- **Regulatory Compliance:** Depending on the industry and location, there might be regulations or compliance standards that require you to keep certain information about your technology infrastructure confidential. Failing to do so could lead to compliance issues and potential fines.

10. **Vulnerability Name:** Microsoft Windows SMB NativeLanManager Remote System

Information Disclosure

Severity : INFO

Plugin: 46215

Port : tcp/0

Description: The remote host's hostname is not consistent with DNS information. The name of this machine either does not resolve or resolves to a different IP address. This may come from a badly configured reverse DNS or from a host file in use on the Nessus scanning host. As a result, URLs in plugin output may not be directly usable in a web browser and some web tests may be incomplete.

Solution: Fix the reverse DNS or host file.

Business Impact: This issue can have significant business impacts:

- **Security Risk:** This problem can allow unauthorized access to your computer systems. It's like leaving a back door open for hackers to get in and potentially steal or damage your business data.
- **Data Breach:** If attackers exploit this vulnerability, they could gain access to sensitive business information, such as customer data, financial records, or intellectual property. This could lead to data breaches, which can harm your business's reputation and result in legal and financial consequences.
- **Downtime and Disruption:** Exploiting this vulnerability can disrupt your computer systems, causing downtime and making it difficult for your employees to work. This can result in lost productivity and revenue.

- Reputation Damage: Security issues can damage your company's reputation, making customers and partners hesitant to do business with you. A damaged reputation can be challenging to recover from.
- Financial Costs: Addressing security vulnerabilities and recovering from attacks can be expensive, involving expenses related to cybersecurity measures, system repairs, and potential legal actions.

STAGE 3 REPORT

Achieving Proactive Cybersecurity with SOC and SIEM Integration

SECURITY OPERATIONS CENTER (SOC)

A Security Operations Center (SOC) is a critical component of an organization's cybersecurity strategy. It's essentially a centralized unit or team responsible for monitoring, detecting, responding to, and mitigating security incidents and threats across an organization's IT infrastructure. Here's a more detailed explanation of SOC:

Purpose and Function:

- **Monitoring:** The primary function of a SOC is to continuously monitor an organization's network, systems, and applications for signs of malicious activities or security anomalies. This monitoring can be proactive, looking for vulnerabilities before they are exploited, or reactive, responding to ongoing incidents.
- **Detection:** SOC analysts use a variety of tools, including Intrusion Detection Systems (IDS), Security Information and Event Management (SIEM) systems, and threat intelligence feeds, to detect and identify potential security threats. They analyze logs, traffic patterns, and behavior to spot unusual or suspicious activities.
- **Incident Response:** When a security incident is identified, the SOC is responsible for responding promptly and effectively. This involves investigating the incident, understanding its scope and impact, containing the threat, and taking necessary actions to mitigate damage and prevent recurrence.
- **Threat Hunting:** Beyond reacting to known threats, some SOC's also engage in proactive threat hunting. This involves actively seeking out hidden or novel threats that might have evaded automated detection systems.

Team Structure:

- **SOC Manager:** Oversees the SOC's operations, including strategy, staffing, and budgeting.
- **Analysts:** Security analysts are the frontline responders. They investigate alerts, assess threats, and execute incident response plans.
- **Threat Hunters:** These analysts proactively search for potential threats within the organization's network and systems.

- **Incident Responders:** Specialized analysts focus exclusively on responding to and mitigating security incidents.
- **Engineers:** These professionals maintain and configure security tools and infrastructure.
- **Security Architects:** They design and implement security solutions and policies.

Tools and Technologies:

- **SIEM Systems:** Security Information and Event Management systems collect, correlate, and analyze data from various sources to identify security events.
- **IDS/IPS:** Intrusion Detection Systems and Intrusion Prevention Systems monitor network traffic for signs of malicious activities and can take automated actions to block threats.
- **Firewalls:** Network firewalls filter incoming and outgoing traffic to prevent unauthorized access.
- **Endpoint Detection and Response (EDR):** EDR tools monitor endpoints (computers, servers, devices) for unusual behavior or malicious activity.
- **Threat Intelligence Feeds:** These provide information on known threats, tactics, techniques, and procedures used by cybercriminals.

Challenges and Considerations:

- **Alert Fatigue:** SOC's often generate numerous alerts, and distinguishing real threats from false alarms can be challenging.
- **Skills Gap:** Skilled cybersecurity professionals are in high demand, making it challenging for organizations to recruit and retain SOC talent.
- **Costs:** Setting up and maintaining an effective SOC can be expensive, from technology investments to personnel costs.
- **Evolving Threat Landscape:** Threats are constantly evolving, and SOC's need to stay updated with the latest attack techniques and vulnerabilities.

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Security Information and Event Management (SIEM) is a security solution that helps organizations detect, investigate, and respond to security threats. It collects and analyzes security logs, network traffic, and other data from a variety of sources, including firewalls, intrusion detection systems, and endpoint security solutions. SIEM uses machine learning and artificial intelligence to identify threats and anomalies, and it provides security analysts with a variety of tools to investigate and respond to incidents.

SIEM is important because it can help organizations to:

- **Detect threats more quickly:** SIEM can collect and analyze data from a variety of sources, which can help organizations to identify threats that may not be obvious to human analysts.
- **Reduce the impact of security incidents:** SIEM can help organizations to respond to incidents more quickly and effectively, which can help to reduce the impact of a breach.
- **Meet compliance requirements:** SIEM can help organizations to comply with a variety of security regulations.
- **Improve security posture:** SIEM can help organizations to get a better understanding of their security posture and identify areas where improvements can be made.

SIEM typically works in the following steps:

- Collect data from a variety of sources.
- Analyze the data for threats and anomalies.
- Generate alerts for potential threats.
- Investigate alerts and take action as needed.
- Store data for future analysis.

Benefits of SIEM:

- **Increased visibility into security threats:** SIEM can provide organizations with a comprehensive view of their security posture by collecting and analyzing data from a variety of sources. This helps organizations to identify threats that may not be obvious to human analysts.
- **Faster threat detection:** SIEM uses machine learning and artificial intelligence to identify threats and anomalies in the data it collects. This allows organizations to detect threats more quickly, which can help to reduce the impact of a breach.
- **Improved incident response:** SIEM provides security analysts with a variety of tools to investigate and respond to incidents. This helps organizations to respond to incidents more quickly and effectively.
- **Reduced risk of compliance violations:** SIEM can help organizations to comply with a variety of security regulations. This can help to protect organizations from fines and penalties.

Challenges of SIEM :

- **The volume of data:** SIEM solutions need to be able to handle the large volume of data that is generated by modern IT environments.

- The complexity of the data: The data that is collected by SIEM solutions can be complex and difficult to analyze.
- **The need for skilled analysts:** SIEM solutions require skilled analysts to be able to effectively investigate and respond to alerts.
- **The cost of SIEM solutions:** SIEM solutions can be expensive to purchase and maintain.

Conclusion

SIEM is a powerful tool that can help organizations to detect, investigate, and respond to security threats. However, it is important to be aware of the challenges of SIEM and to select a solution that is appropriate for the organization's needs.

IBM QRADAR

IBM QRadar is a Security Information and Event Management (SIEM) platform that helps organizations detect, investigate, and respond to security threats. It collects and analyzes security logs, network traffic, and other data from a variety of sources, including firewalls, intrusion detection systems, and endpoint security solutions. QRadar uses machine learning and artificial intelligence to identify threats and anomalies, and it provides security analysts with a variety of tools to investigate and respond to incidents.

Key features of IBM QRadar:

Collects and analyzes data from a variety of sources: QRadar can collect data from a wide range of security devices and applications, including firewalls, IDS/IPS, SCADA systems, cloud infrastructure, and endpoint security solutions. This allows organizations to get a comprehensive view of their security posture and identify threats that may be coming from multiple sources.

Uses machine learning and artificial intelligence to identify threats: QRadar uses machine learning and artificial intelligence to identify threats and anomalies in the data it collects. This allows it to detect threats that may not be obvious to human analysts.

Provides security analysts with a variety of tools to investigate and respond to incidents: QRadar provides security analysts with a variety of tools to investigate and respond to incidents. These tools include a graphical user interface, a command-line interface, and a variety of pre-built reports and dashboards.

Is available on-premises or as a cloud service: QRadar is available on-premises or as a cloud service. This gives organizations the flexibility to choose the deployment option that best meets their needs.

IBM QRadar is a powerful SIEM platform that can help organizations detect, investigate, and respond to security threats. It is a popular choice for organizations of all sizes, and it has been recognized by industry analysts as a leading SIEM solution.

Benefits of using IBM QRadar:

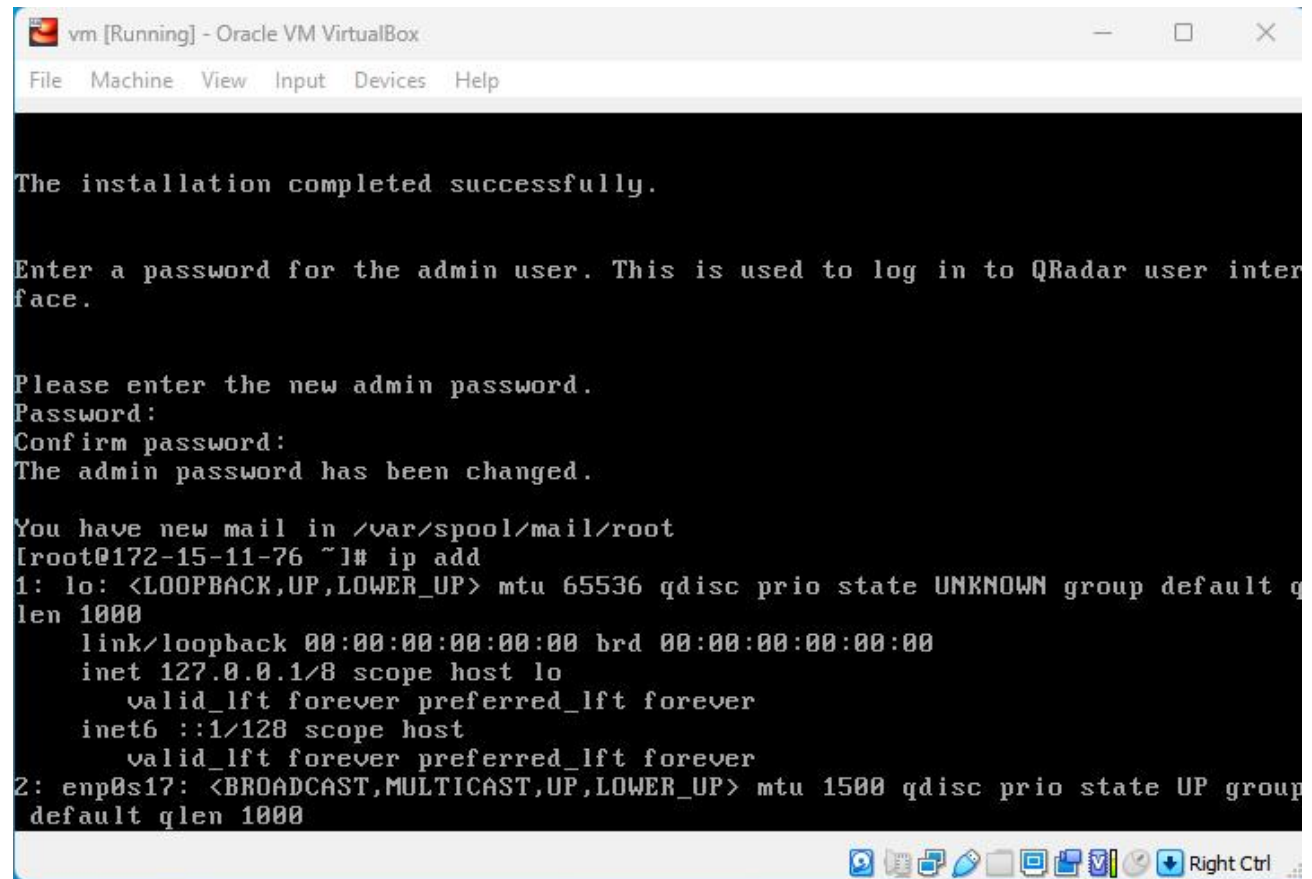
Increased visibility into security threats: QRadar provides organizations with a comprehensive view of their security posture by collecting and analyzing data from a variety of sources. This helps organizations to identify threats that may not be obvious to human analysts.

Faster threat detection: QRadar uses machine learning and artificial intelligence to identify threats and anomalies in the data it collects. This allows organizations to detect threats more quickly, which can help to reduce the impact of a breach.

Improved incident response: QRadar provides security analysts with a variety of tools to investigate and respond to incidents. This helps organizations to respond to incidents more quickly and effectively.

Reduced risk of compliance violations: QRadar can help organizations to comply with a variety of security regulations. This can help to protect organizations from fines and penalties.

Implementation Screenshots:



The screenshot shows a terminal window titled "vm [Running] - Oracle VM VirtualBox". The terminal output indicates a successful installation, followed by a password prompt for the admin user. The user enters a password, and the system confirms the password change. Subsequently, the user checks for new mail and then configures the network interface 'lo' with the IP address 127.0.0.1. The configuration for 'lo' includes setting the MTU to 65536, the QoS discipline to 'prio', and the state to 'UNKNOWN'. The configuration for 'enp0s17' is also shown, with an MTU of 1500 and a state of 'UP'.

```
vm [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

The installation completed successfully.

Enter a password for the admin user. This is used to log in to QRadar user interface.

Please enter the new admin password.
Password:
Confirm password:
The admin password has been changed.

You have new mail in /var/spool/mail/root
[root@172-15-11-76 ~]# ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc prio state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s17: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc prio state UP group default qlen 1000
```

vm [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

The admin password has been changed.

You have new mail in /var/spool/mail/root

[root@172-15-11-76 ~]# ip add

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc prio state UNKNOWN group default qlen 1000

link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00

inet 127.0.0.1/8 scope host lo

valid_lft forever preferred_lft forever

inet6 ::1/128 scope host

valid_lft forever preferred_lft forever

2: enp0s17: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc prio state UP group default qlen 1000

link/ether 08:00:27:18:7c:ba brd ff:ff:ff:ff:ff:ff

inet 172.15.11.76/19 brd 172.15.31.255 scope global enp0s17

valid_lft forever preferred_lft forever

inet6 fe80::a00:27ff:fe18:7cba/64 scope link

valid_lft forever preferred_lft forever

3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default

link/ether 02:42:6e:37:ea:01 brd ff:ff:ff:ff:ff:ff

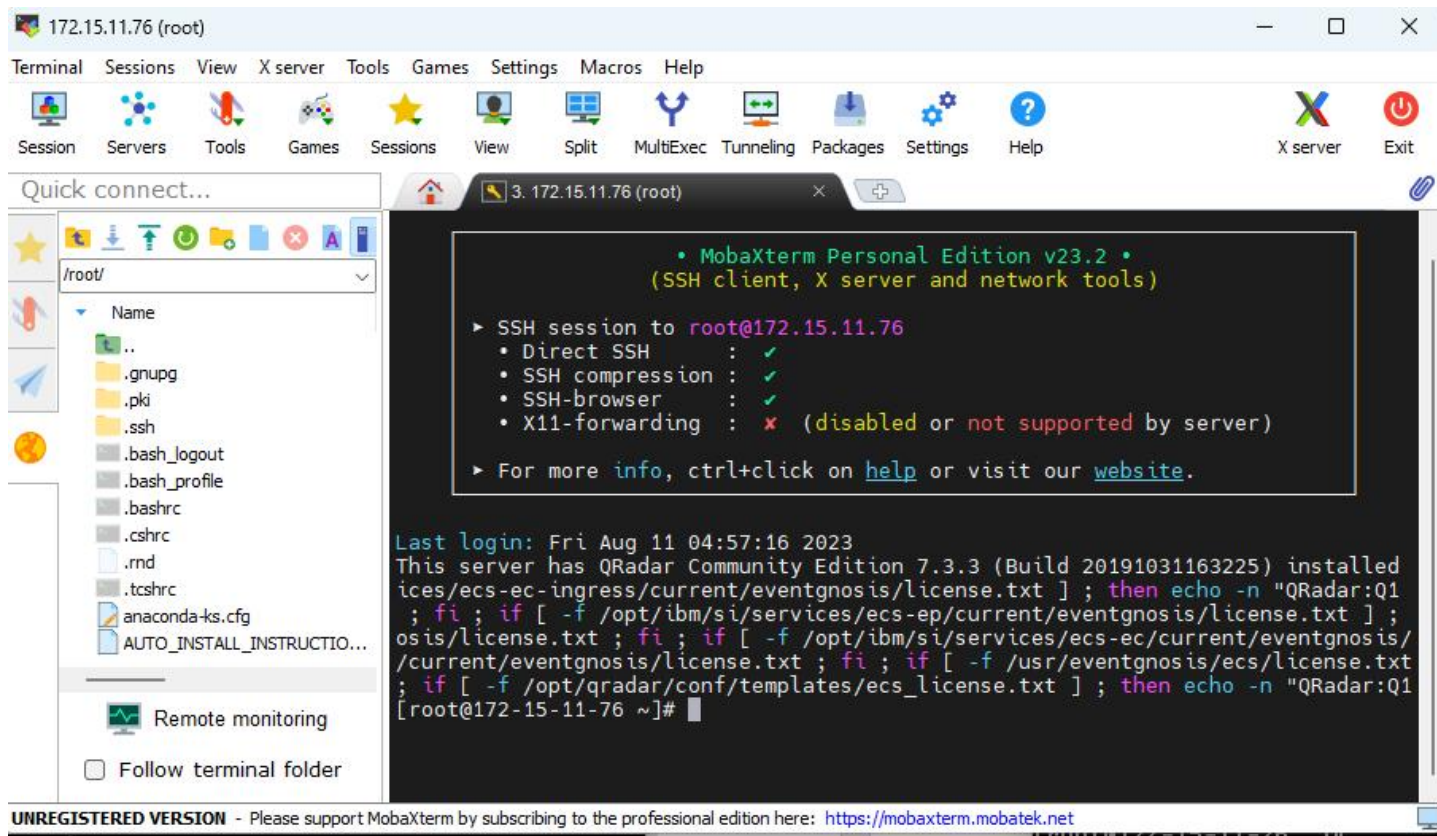
inet 169.254.2.1/24 brd 169.254.2.255 scope global docker0

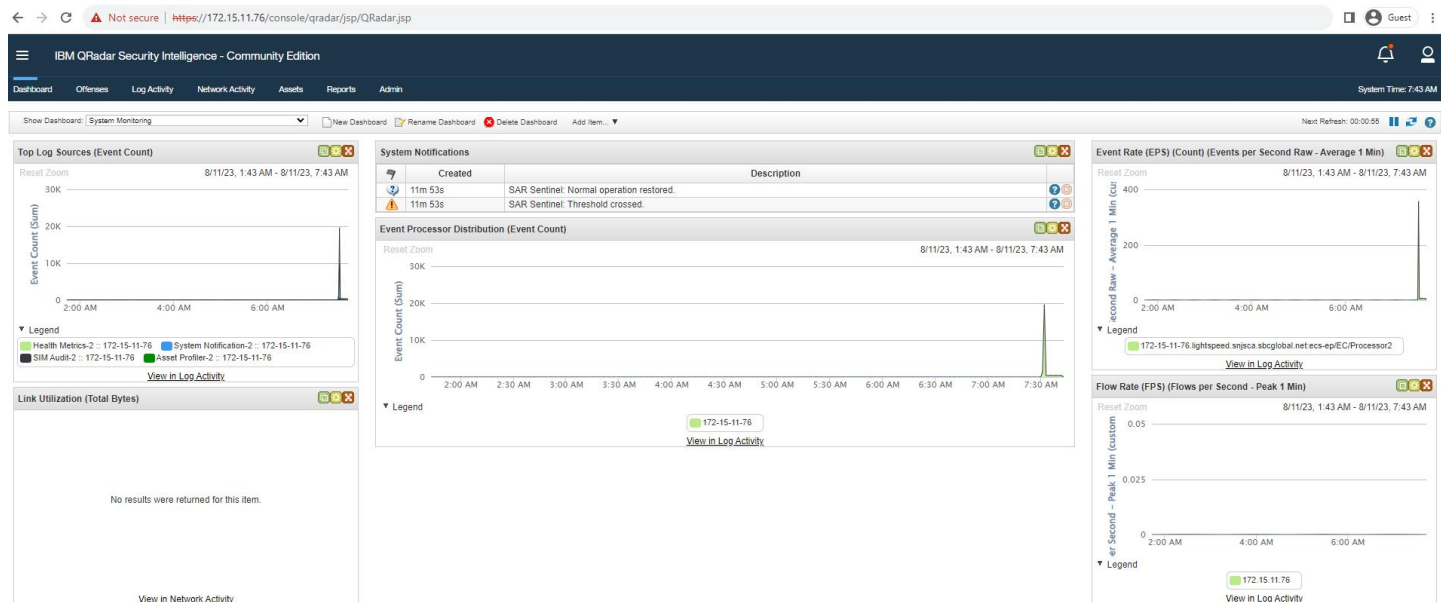
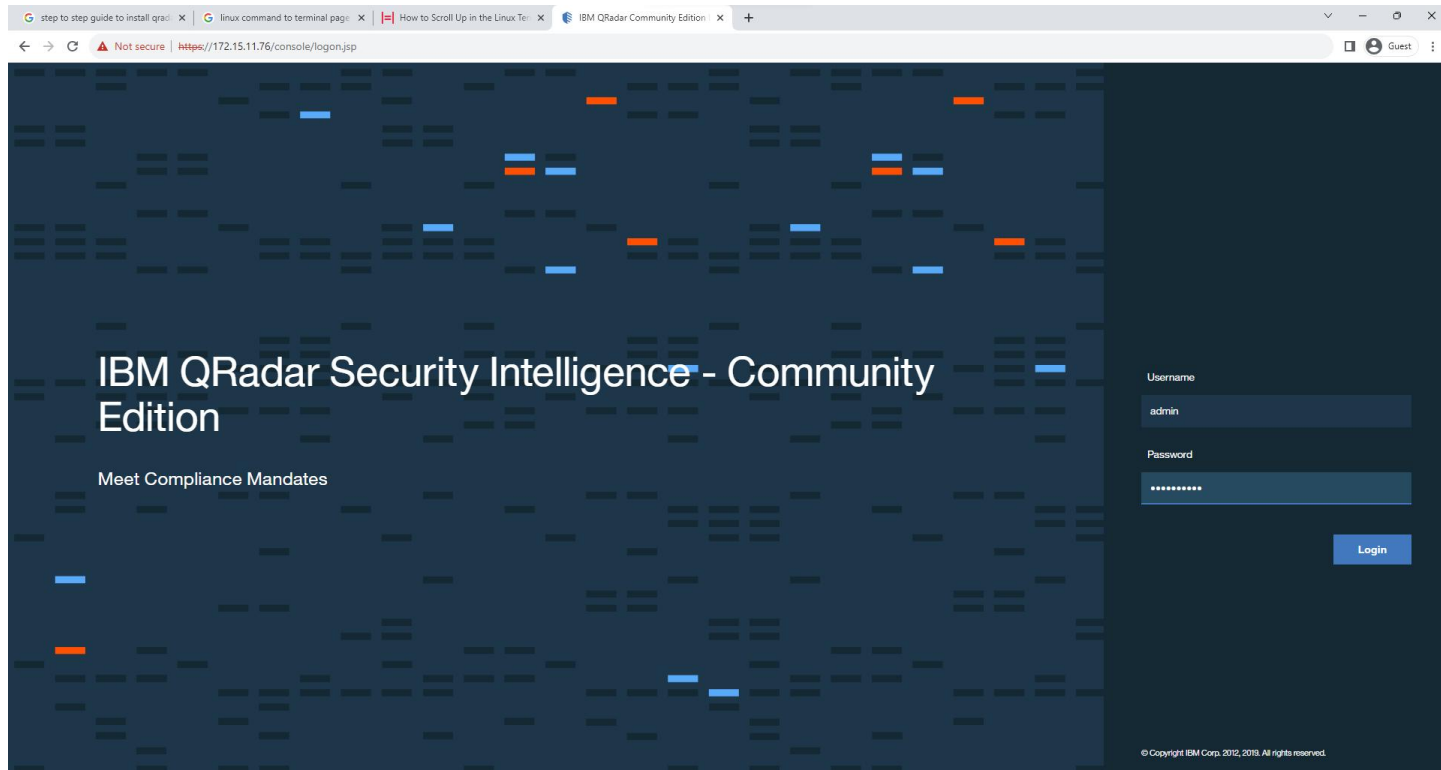
valid_lft forever preferred_lft forever

inet6 2001:db8:4::1/80 scope global

valid_lft forever preferred_lft forever

Right Ctrl







Search... Quick Searches Add Filter Save Criteria Save Results Cancel False Positive Rules Actions

Quick Filter

Start Time 8/11/2023 1:53 AM End Time 8/11/2023

View: Select An Option: Display: High Level Category

Grouping By:

High Level Category

Current Filters:

Event Is Unparsed is False (Clear Filter)

Using Search: Event Category Distribut

Top 10 High Level Category Results By Event Count (Sum)

Reset Zoom

8/11/23, 1:53 AM - 8/11/23, 7:53 AM



Legend

System SIM Audit

Update Details

(Hide Charts)

CONCLUSION

Stage 1 :- what you understand from Web application testing .

The outcome of web application testing is to ensure that the application is secure, reliable, and meets its intended functionality. The testing process aims to identify and address potential vulnerabilities, bugs, and usability issues that could impact the application's performance and user experience.

The specific outcomes of web application testing include:

- Identification of Security Vulnerabilities
- Bug Detection and Resolution
- Validation of Functional Requirements
- Usability and User Experience Evaluation
- Performance and Load Testing Results
- Compatibility Testing Insights
- Accessibility Compliance
- Security Compliance and Risk Mitigation
- Optimization Recommendations
- Enhanced Quality Assurance
- Increased Customer Confidence
- Compliance with Regulatory Requirements

In summary, the outcome of web application testing is an enhanced, secure, and reliable web application that meets user expectations and delivers a smooth and seamless experience to its users. It provides developers and stakeholders with the confidence that the application is ready for deployment and can withstand potential security threats and performance challenges.

Stage 2 :- what you understand from the nessus report.

Nessus is a vulnerability scanning tool used to identify and report security issues in computer systems and networks. The outcome of a Nessus report will depend on the specific target scanned and the vulnerabilities found. Typically, a Nessus report will list the identified vulnerabilities along with their severity levels, detailed descriptions, and recommendations for remediation. The severity levels are usually categorized as critical, high, medium, and low, depending on the potential impact and exploitability of the vulnerability.

Stage 3 :- what you understand from SOC / SEIM / Qradar Dashboard.

SOC (Security Operations Center): The primary purpose of a SOC is to monitor and defend an organization's IT infrastructure against security threats and incidents. SOC analysts use various tools and technologies to detect, analyze, and respond to security events in real-time. The expected outcomes of a well-functioning SOC include:

- a. Improved Threat Detection:** SOC analysts monitor network traffic, log data, and security alerts to identify potential threats and security incidents promptly.
- b. Faster Incident Response:** With a SOC in place, organizations can respond quickly to security incidents and mitigate the impact of breaches or attacks.
- c. Enhanced Security Posture:** A proactive SOC helps organizations implement robust security measures and continually improve their overall security posture.
- d. Reduced Downtime and Losses:** Detecting and mitigating security incidents swiftly can minimize downtime and financial losses resulting from cyber-attacks.

SIEM (Security Information and Event Management): SIEM is a technology that helps collect, analyze, and correlate log data from various sources within an organization's IT environment. The main goal of SIEM is to provide a centralized platform for real-time monitoring, threat detection, and incident response. The expected outcomes of using a SIEM system are:

- a. Centralized Log Management:** SIEM aggregates log data from diverse sources, making it easier for analysts to access and analyze information from a single dashboard.
- b. Early Threat Detection:** SIEM tools can identify patterns and anomalies in the data, enabling early detection of security incidents and potential breaches.
- c. Simplified Incident Investigation:** SIEM allows analysts to correlate events from different sources, providing a comprehensive view of security incidents for faster and more accurate investigations.
- d. Compliance and Reporting:** SIEM can help organizations meet regulatory compliance requirements by generating security reports and audits.

QRadar Dashboard (IBM QRadar): QRadar is a popular SIEM solution provided by IBM. The QRadar dashboard is a critical component of the QRadar system, offering a visual representation of security-related data and insights. The expected outcomes of using QRadar and its dashboard include:

- a. Real-Time Visibility:** The QRadar dashboard provides real-time visibility into security events and incidents, enabling analysts to respond promptly to emerging threats.
- b. Customizable Visualizations:** Analysts can customize the dashboard to display relevant information, such as top threats, network traffic, or security incidents.

c. Threat Intelligence Integration: QRadar integrates with various threat intelligence feeds, enhancing its ability to detect and respond to advanced threats.

d. Incident Response Automation: The QRadar dashboard can be integrated with automation tools to streamline incident response processes. It's important to note that the effectiveness of these security measures relies on the expertise of the security team, the quality of data collected, and the organization's commitment to maintaining a strong security posture. Continuous monitoring, analysis, and improvement are crucial for maximizing the outcomes and benefits of SOC, SIEM, and QRadar implementations.

FUTURE SCOPE

Stage 1 :- Future scope of web application testing

The future scope of web application testing will be shaped by technological advancements, changing user expectations, and the need to ensure security and reliability in an increasingly interconnected digital world. Testing professionals will need to adapt to these trends and continuously upgrade their skills to meet the evolving demands of web application testing.

Stage 2 :- Future scope of testing process you understood.

The future scope of the testing process will see increased automation, integration with emerging technologies, and a focus on ensuring quality, security, and performance in the ever-evolving software landscape. Testing professionals will need to adapt to these changes and continuously upgrade their skills to stay relevant in the dynamic field of software testing.

Stage 3 :- future scope of SOC / SEIM

The future scope of SOC (Security Operations Center) and SIEM (Security Information and Event Management) is expected to expand and evolve in response to the changing cybersecurity landscape and technological advancements. The future scope of SOC and SIEM will involve increased automation, advanced threat detection, integration with emerging technologies, and a proactive approach to cybersecurity. Organizations will need to invest in the latest tools and technologies while continuously developing the expertise of their cybersecurity teams to stay ahead of evolving threats.

Topics explored :-

Introduction to cybersecurity, Growth of cybersecurity, Data sanity, Cloud service and cloud security, Data breach, Firewall, Antivirus, Digital ecosystem, Data protection, Types of cyber attacks, Essential terminology, Introduction to networking, Web APIs, web hooks, Web shell concepts, Vulnerability stack, OWASP top 10 applications, QRadar, SOC, SIEM

Tools explored :-

Nessus, OWASP top 10 vulnerabilities(2021), thehackersnews.com, CWE, exploitDB, virtual box, live websites-bugcrowd, nslookup.io, OSINT framework, mitre framework, IBM fix central, QRadar Installation, mobaxterm, tools-nmtui, Nmap, sqlmap, Identify fixes-wincollect agent, metasploitable, malware bytes, Linux cheatsheet, QRadar for SOC dashboard presentation, Kali linux.